

549423

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004年10月7日 (07.10.2004)

PCT

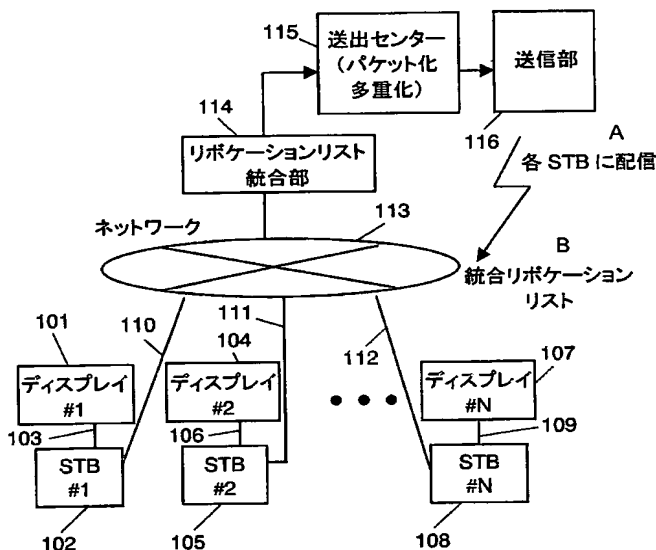
(10) 国際公開番号
WO 2004/086235 A1

- (51) 国際特許分類⁷: G06F 12/14, H04N 7/16 (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 鈴木 秀和 (SUZUKI, Hidekazu).
- (21) 国際出願番号: PCT/JP2004/004138
- (22) 国際出願日: 2004年3月25日 (25.03.2004) (74) 代理人: 岩橋 文雄, 外(IWAHASHI, Fumio et al.); 〒5718501 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内 Osaka (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (30) 優先権データ:
特願2003-085043 2003年3月26日 (26.03.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1 0 0 6 番地 Osaka (JP).

[続葉有]

(54) Title: REVOCATION INFORMATION TRANSMISSION METHOD, RECEPTION METHOD, AND DEVICE THEREOF

(54) 発明の名称: リボケーション情報の送信方法、受信方法及びその装置



- 115...TRANSMISSION CENTER (PACKETIZING, MULTIPLEXING)
116...TRANSMISSION SECTION
114...REVOCATION LIST INTEGRATION SECTION
113...NETWORK
101...DISPLAY #1
104...DISPLAY #2
107...DISPLAY #N
A...DISTRIBUTION TO EACH STB
B...INTEGRATED REVOCATION LIST

(57) Abstract: There are provided a revocation information transmission method, a revocation information reception method, a revocation information transmission device, and a revocation information reception device capable of causing all the video output devices such as an STB to share a revocation list, excluding an unauthorized display, and improving the security of the digital interface connecting the video output device to the display. The revocation information transmission method includes at least a step of integrating the revocation information in the content transmission device or content reception device so as to create integrated revocation information, a step of packetizing the integrated revocation information and multiplexing it on the stream, and a step of transmitting the stream.

(57) 要約: リボケーションリストをSTB等の全ての映像出力機器に共有させることができ、不正なディスプレイを排除することが可能で、且つ映像出力機器とディスプレイとを接続するデジタルインタフェースのセキュリティを向上させることができるリボケーション情報の送信方法、リボケーション情報の受信方法、リボケーション情報の送信装置、及びリボケーション情報の受信装置が提供される。このリボケーション情報の送信方法は、少なくとも、コンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合して統合リボケーション情報を作成するステップと、統合リボケーション情報をパケット化しストリームに多重するステップと、ストリームを送出するステップとを備え

WO 2004/086235 A1

る。



(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 国際調査報告書
- 補正書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

リポケーション情報の送信方法、受信方法及びその装置

技術分野

- 5 この発明は、デジタル映像やデジタル音声を不当な電子機器で表示したり、再生したりすることを防止するためのリポケーション情報の配信方法及び装置に関するものである。

背景技術

- 10 近年、デジタル技術の発展に伴って、デジタル放送やインターネットによるデジタルコンテンツの配信や、DVDやハードディスクやメモリカードによるデジタルコンテンツの配布や蓄積が盛んに行なわれている。これらのメディアではデジタルデータが用いられているので、その品質を劣化させることなくコピーを行なうことが可能である。し
15 かし、著作権保護の観点からその不正なコピーを防ぐためのセキュリティの実現が重要である。セキュリティの実現のためには、著作権保護上、不正な機器が発覚した場合、不正機器のいわゆるブラックリストであるリポケーション情報が発行される必要がある。そうして、不正な機器に接続されうる機器がそのリポケーション情報を持ち、デジ
20 タルコンテンツへの不正なアクセスを防ぐ必要がある。

図31はリポケーション情報の更新に関する従来例のシステムの構成を図25に示す。このような構成は、特開2001-166996号公報に開示されている。

- 25 コンテンツ販売システム3001は、放送やインターネットの通信網を介して音楽コンテンツを電子配信する自動販売機である。Electric MUSIC Distributer（図31ではEMDと記載し、以降の説明でもEMDと記載する）3002は音楽サー

- パーや音楽放送局である。リボケーション情報発行機関 3003 はリボケーション情報を発行する。リボケーション情報格納部 3005 は、リボケーション情報発行機関 3003 が発行したリボケーション情報を受け取る。音楽データ格納部 3006 は、音楽データを格納する。
- 5 ライセンス格納部 3007 は、暗号化コンテンツを復号するためのキーを格納する。EMD I/F 部 3008 は、暗号化コンテンツを受け取るためのインタフェースである。PD I/F 部 3009 は、記録再生装置 (PD) 3012 と接続するためのインタフェースである。
- 10 メディア I/F 部 3010 は、記録メディア 3014 を装着するための PCMCIA のカードスロットである。記憶メディア 3014 は、Portable Media (PM) である。記憶再生装置 3012 は記録メディア 3013 を装着する。ユーザ I/F 部 3011 はユーザが操作を行うインタフェースである。セキュアコンテンツサーバー 3004 はサーバーであり、EMD I/F 部 3008、リボケーション情報格納部 3005、音楽データ格納部 3006、ライセンス格納部 3007、メディア I/F 部 3010、ユーザ I/F 部 3011、及び PD I/F 部 3009 との間で情報授受をする。
- 15

発明の開示

- 20 リボケーション情報の送信方法は、
- コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、コンテンツ送出機器とコンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、
- コンテンツ送出機器とコンテンツ受信機器が相互認証を行なう
- 25 ステップと、
- 相互認証が失敗の場合、コンテンツ送出機器またはコンテンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーション情報

をアップロードするステップと、

アップロードされた個々のリポケーション情報を統合して統合リポケーション情報を作成するステップと、

5 統合リポケーション情報をパケット化し、ストリームに多重するステップと、

ストリームを送出するステップと
を備える。

リポケーション情報の送信方法は、

1 個または複数のコンテンツ送出機器またはコンテンツ受信機器
10 のリポケーション情報を統合して統合リポケーション情報を作成するステップと、

統合リポケーション情報をパケット化し、ストリームに多重するステップと、

ストリームを送出するステップと
15 を備える。

リポケーション情報の受信方法は、

コンテンツ送出機器またはコンテンツ受信機器が統合リポケーションリストを受信するステップと、

コンテンツ送出機器またはコンテンツ受信機器が統合リポケーションリストを記憶するステップと
20 を備える。

リポケーション情報の送信装置は、

コンテンツを送出する複数のコンテンツ送出機器と、

複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、
25

コンテンツ送出機器とコンテンツ受信機器とを接続する接続手段と、

複数のコンテンツ送出機器または複数の受信機器からリボケーション情報を吸い上げるネットワークと

ネットワークに接続され、リボケーション情報を統合する統合手段と、

5 統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、

ストリームを送信する送信手段と
を備える。

リボケーション情報の送信装置は、

10 1個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合する統合手段と、

統合リボケーション情報をパケット化してストリームに多重する多重化手段と、

ストリームを送信する送信手段と

15 を備える。

リボケーション情報の受信装置は、

統合リボケーションリストを受信するコンテンツ送出機器またはコンテンツ受信機器を備え、

20 コンテンツ送出機器またはコンテンツ受信機器は統合リボケーションリストを記憶する。

図面の簡単な説明

図1は実施の形態1～3におけるリボケーションリストの送信方法、受信方法を実現するシステムを示す図である。

25 図2はディスプレイの内部構成を示す図である。

図3は実施の形態1～3におけるSTBの内部構成を示す図である。

図4はデバイスキーの行列を示す図である。

図 5 は初期認証の処理を示す図である。

図 6 は S T B が持つリボケーションリストの一例を示す図である。

図 7 は S T B が持つリボケーションリストの作成のフローを示す図である。

5 図 8 は更新されたりボケーションリストの一例を示す図である。

図 9 は実施の形態 1 ～ 3 におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図である。

図 10 はトランスポートパケットのデータ構造を模式的に示す図である。

10 図 11 はトランスポートパケットのデータ構造を示す図である。

図 12 は統合リボケーションリストをセクション構造に格納した場合のデータ構造を示す図である。

図 13 は実施の形態 1 の統合リボケーションリストの受信フローを示す図である。

15 図 14 は各 S T B で共有される統合リボケーションリストの一例を示す図である。

図 15 は S T B が持つリボケーションリストの一例を示す図である。

図 16 は更新されたりボケーションリストの一例を示す図である。

20 図 17 は統合リボケーションリストをセクション構造に格納した場合のデータ構造の一例を示す図である。

図 18 は各 S T B で共有される統合リボケーションリストの一例を示す図である。

図 19 は統合リボケーションリストを P E S パケット構造に格納した場合のデータ構造を示す図である。

25 図 20 は実施の形態 2 における統合リボケーションリストの受信フローを示す図である。

図 21 は統合リボケーションリストを P E S パケット構造に格納し

た場合のデータ構造の一例を示す図である。

図 2 2 は統合リボケーションリストをトランスポートパケットのペイロードに格納した場合のデータ構造の一例を示す図である。

5 図 2 3 は実施の形態 3 における統合リボケーションリストの受信フローを示す図である。

図 2 4 は統合リボケーションリストをトランスポートパケットのペイロードに格納した場合のデータ構造を示す図である。

図 2 5 は実施の形態 4 におけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図である。

10 図 2 6 は実施の形態 4 における S T B の内部構成を示す図である。

図 2 7 は実施の形態 4 におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図である。

図 2 8 は I P パケットのデータ構造を示す図である。

15 図 2 9 は実施の形態 4 における統合リボケーションリストの受信フローを示す図である。

図 3 0 は実施の形態 5 おけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図である。

図 3 1 は従来例を示す図である。

20 発明を実施するための最良の形態

上述の従来例ではリボケーション情報の更新方法については述べられているが、リボケーション情報を配信する具体的方法がない。そのため、デジタル放送やインターネットでのコンテンツ配信が高まりを見せる状況で、リボケーション情報の配信するための方法が必要である。

25 (実施の形態 1)

以下、図面を参照しながら本発明の実施の形態 1 について説明する。

図 1 は本発明におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す図である。第 1 のディスプレイ 1 0 1 (図 1 ではディスプレイ # 1 と記載する) は、C R T や液晶ディスプレイやプラズマディスプレイ等であって、映像を表示する。第 1 のディスプレイ 1 0 1 は、スピーカも備え音声を出力する場合もある。

図 2 は第 1 のディスプレイ 1 0 1 の内部構成を示す。表示部 1 0 0 1 は映像を表示する。機器インタフェース 1 0 0 2 は後述する S T B と接続する為のものである。ディスプレイのコントロール部 1 0 0 3 は、ディスプレイ全体の制御を行う。メモリ部 1 0 0 4 は、後述するディスプレイのメーカ I D や機器 I D や鍵情報を格納する。

第 1 の S T B (図 1 では S T B # 1 と記載する。また、S T B はセットトップボックスのことである。) 1 0 2 は、配信または放送されるデジタルの映像や音声その他のデータを受信し、復号し、再生を行う。ここではデジタル放送を受信する S T B とする。

図 3 はその S T B の内部構成を示す。アンテナ 1 1 0 1 はデジタル放送の電波を受信する。チューナー部 1 1 0 2 は、放送波の復調を行う。フロントエンド部 1 1 0 3 は、復調された信号に対して誤り訂正等を行って T S (トランスポートストリーム) を再生する。T S デコーダ部 1 1 0 4 は、複数の番組が多重された T S からユーザが選択した番組のパケット (映像、音声、データ等) を抽出する。A V デコーダ部 1 1 0 5 は、T S デコーダ部 1 1 0 4 で抽出した映像パケット及び音声パケットの伸張を行い、デジタルの映像信号及び音声信号を出力する。コントロール部 1 1 0 6 は、S T B の全体の制御を行う。メモリ部 1 1 0 7 は、後述するリボケーションリストや S T B の鍵情報など格納する。ディスプレイインタフェース 1 1 0 8 は映像や音声をディスプレイに向けて出力したり、鍵情報を交換したりする。モデム部 1 1 0 9 は、後述するネットワーク 1 1 3 と通信する。

デジタルインタフェース 103 は第 1 のディスプレイ 101 と第 1 の STB 102 とを接続するデジタルインタフェースであり、ここでは例として HDMI (High-Definition Multimedia Interface) とする。第 2 のディスプレイ 104 (図 1 ではディスプレイ # 2 と記載する) は、第 1 のディスプレイ 101 と同様なものである。第 2 の STB (図では STB # 2 と記載する) 105 は、第 1 の STB 102 と同様なものである。第 2 のデジタルインタフェース 106 は第 2 のディスプレイ 104 と第 2 の STB 105 を接続するデジタルインタフェースで、第 1 のデジタルインタフェース 103 と同一である。

第 N のディスプレイ (N は自然数、図 1 ではディスプレイ # N と記載する) 107 は、第 1 のディスプレイ 101 と同様なものである。第 N の STB (図 1 では STB # N と記載する) 108 は、第 1 の STB 102 と同様なものである。第 N のデジタルインタフェース 109 は、第 1 のデジタルインタフェース 103 と同様なものである。

第 1 の上り回線 110 は第 1 の STB 102 と後述するネットワークとを接続する。これは、STB に蓄積されたりボケーションリストをネットワークに送信するための媒体である。リボケーションリストについては後で説明する。上り回線には銅線や光ケーブル等がある。

第 2 の上り回線 111 は、第 1 の上り回線 110 と同様なものである。第 N の上り回線 112 は、第 1 の上り回線 110 と同様なものである。参照符号 101 ~ 112 が付された部分は各家庭に存在するものまたは、各家庭個別に対応するものである。また、N の値は限定されるものではない。

ネットワーク 113 は、各家庭の STB からリボケーションリストをリボケーションリスト統合部 114 に吸い上げるための媒体であり、例えば電話網やインターネットなどである。リボケーションリスト統

合部 1 1 4 は各 S T B から吸い上げられたリボケーションリストを統合して、リボケーションリストの一覧である統合リボケーションリストの作成及び管理を行う。送出センター 1 1 5 は、統合されたりボケーションリストをパケット化して放送用のトランスポートストリーム
5 に多重する。送信部 1 1 6 は、これらの情報などを各 S T B に送信する。送信部 1 1 6 は、例えば送信アンテナなども備えている。

以上のように構成された実施の形態 1 についてその動作を説明する。H M D I ではコンテンツ保護のため H D C P (H i g h - B a n d w
i d t h D i g i t a l C o n t e n t P r o t e c t i o
10 n) という暗号化システムが用いられる。H D C P は、S T B や D V D プレーヤ、D V D レコーダといった映像や音声を送出する送出機器と、ディスプレイなど映像を表示する受信機器との間に流れるデジタルコンテンツの暗号化方法を規定する。詳細は H D C P の規格書である、H i g h - B a n d w i d t h D i g i t a l C o n t e n
15 t P r o t e c t i o n S y s t e m、に詳述されており説明を省略する。

第 1 のディスプレイ 1 0 1 ~ 第 N のディスプレイ 1 0 7 は、それぞれのメモリ部 1 0 0 4 に、メーカー I D、機器 I D 及び 5 6 ビット × 4 0 行のディスプレイ用のデバイスキーの行列を有している。図 4 は
20 この様子を示す。また、このデバイスキーの行列に対応して、個々のデバイスキーの行を指定するためのキーセレクションベクトル（以下 K S V と略す）が割り当てられ、メモリ部 1 0 0 4 に格納されている。以降、ディスプレイ用の K S V を B k s v と記す。

また第 1 の S T B 1 0 2 ~ 第 N の S T B 1 0 8 もそれぞれのメモリ
25 部 1 1 0 7 に S T B 用のデバイスキーと K S V を有している。以降、S T B 用の K S V を A k s v と記す。

デバイスキーもキーセレクションベクトルも、H D C P の管理組織で

あるLLCが管理し、各ディスプレイやSTBやDVDといった各機器に付与する。

次に各STBでのリボケーションリストの作成の方法について説明する。例として、第1のSTB102と第1のディスプレイ101について説明する。図5にSTBとディスプレイの初期認証の処理を示す。この処理の詳細は先述した文献High-Bandwidth Digital Content Protection Systemに述べられており、説明を省略する。図6は、第1のSTB102のメモリ部1107が有しているリボケーションリストの例を示す。

このリストには、著作権保護上、不正機器として排除すべきディスプレイのメーカーID、機器ID、Bksvが格納されている。図6の例では2個のディスプレイが排除されるべき機器として登録されている。メーカーIDはメーカを識別するものである。機器IDは機器を識別するもので例えば機器のシリアルナンバーである。

以下、初期認証について説明する。まず、第1のSTB102と第1のディスプレイ101が第1のデジタルインタフェース103で接続されるか、または第1のSTB102と第1のディスプレイ101に電源が投入される。

次に第1のSTB102は第1のディスプレイ101からメーカーID、機器ID、Bksvを第1のデジタルインタフェース103を介して読み出す。このとき、第1のデジタルインタフェース103の制御線であるI2Cラインを用いればよい。

ここで、読み出したメーカーID、機器ID、Bksvが第1のSTB102が持っているリボケーションリストと同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

次に、第1のSTB102から第1のディスプレイ101に対して、64ビットの乱数Anと、Aksvが第1のデジタルインタフェース

1 0 3 経由で書き込まれる。

ここでも I 2 C ラインを用いればよい。

次に、第 1 の S T B 1 0 2 は第 1 のディスプレイ 1 0 1 から B k s v を読み出し、第 1 の S T B 1 0 2 で、下記 (式 1) の演算を行なう。

$$5 \quad K_m = \sum A_{keys} \text{ over } B_{ksv} \quad (\text{式 1})$$

(式 1) の演算を説明する。A k e y s は S T B のメモリ部 1 1 0 7 に格納されている 5 6 ビット×4 0 行の S T B のデバイスキーの行列である。例えば B k s v を 1 6 進数表現で「2 B 8」とし、最初のビット位置を 0 番目とすると、ビット位置 3, 4, 5, 7, 9 は「1」であり、それ以外のビット位置では「0」である。

そして、(式 1) は B k s v の「1」が存在するビット位置 3, 4, 5, 7, 9 を行のインデクスとして、5 個の 5 6 ビットのキーを加算したものである。

第 1 のディスプレイ 1 0 1 でも、同様に (式 2) の演算が行なわれる。

$$15 \quad K_m' = \sum B_{keys} \text{ over } A_{ksv} \quad (\text{式 2})$$

B k e y s はディスプレイのメモリ部 1 0 0 4 に格納されている 5 6 ビット×4 0 行のディスプレイのデバイスキーの行列である。

次に第 1 の S T B 1 0 2 は K_m をもとにして (式 3) の演算を行ない、K s、M 0、R 0 を得る。

$$20 \quad (K_s, M_0, R_0) = \text{hdcpBlkCipher}(K_m, \text{REPEATER} \parallel A_n) \quad (\text{式 3})$$

(式 3) で R E P E A T E R は該当する機器がリピート機能、つまり再送信機能を果たす場合に「1」で、それ以外の場合は「0」である。ここではディスプレイがリピート機能を有さないとし、R E P E A T E R を「0」とする。また (式 3) で \parallel はビットの連結を示す。

(式 3) で用いられる h d c p B l k C i p h e r という演算子については、文献 H i g h - B a n d w i d t h D i g i t a l C o

Content Protection Systemの4. 5節に詳述されているので説明を省略する。

一方、第1のディスプレイ101でも同様に(式4)の演算を行なう。

$$\begin{aligned} & (Ks', M0', R0') \\ & = \text{hdcpBlkCipher}(Km', \text{REPEATER} || An) \quad (\text{式4}) \end{aligned}$$

次に初期認証の判定処理が行なわれるが、図7はこの様子を示す。STBはディスプレイから $R0'$ を読み出し、 $R0 = R0'$ であるかどうかを判定する。もし $R0$ と $R0'$ が一致すれば、初期認証は成功である。一方、 $R0$ と $R0'$ が一致しなければ、初期認証は失敗とし、第1のSTB102はディスプレイの $Bksv$ は違反しているものとしてメモリ部1107のリボケーションリストに登録する。このとき、STBはメーカーIDと機器IDも併せて格納する。図8はその場合のメモリ部1107の様子を示す。図8において、 $maker_3$ 、 $kiki_3$ 、 $Bksv_3$ が新たな不正機器として登録された機器である。

以上の初期認証処理の詳細は文献High-Bandwidth Digital Content Protection Systemに詳述されているので説明を省略する。第2のSTB105～第NのSTB108、第2のディスプレイ104～第Nのディスプレイ107も、第1のSTB102、第1のディスプレイ101と同様な初期認証処理を行ない、違反している $Bksv$ があれば、それらに接続されたSTBのメモリ部のリボケーションリストに登録する。

次に各STBに登録されているリボケーションリストを統合して、各STBに送信する方法について説明する。図9にリボケーションリストのアップロード～送出までのフローを示す。

ステップ101において、

S T B のコントロール部 1 1 0 6 が、メモリ部 1 1 0 7 に格納されたりボケーションリストからメーカー I D、機器 I D、Bksv を読み出し、モデム部 1 1 0 9 に転送する。

ステップ 1 0 2 において、

- 5 S T B のモデム部 1 1 0 9 から上り回線 1 1 0、ネットワーク 1 1 3 経由で Bksv がリボケーションリスト統合部 1 1 4 にアップロードされる。

ステップ 1 0 3 において、

- 10 リボケーションリスト統合部 1 1 4 には、所定期間に各 S T B からアップロードされた Bksv のリストを作成し、これを統合力ボケーションリストとする。

ステップ 1 0 4 において、

リボケーションリスト統合部 1 1 4 から送出センター 1 1 5 に統合力ボケーションリストが伝送される。

- 15 ステップ 1 0 5 において、

送出センター 1 1 5 は統合力ボケーションリストをパケット化して、トランスポートストリームに多重する。

ステップ 1 0 6 において、

- 20 送信部 1 1 6 は、統合力ボケーションリストが多重されたトランスポートストリームを各 S T B に送信する。

ここでステップ 1 0 5 におけるリボケーションリストのパケット化及び多重化について詳細に説明する。図 1 0 はトランスポートパケットの模式図を示し、図 1 1 はトランスポートパケットのデータ構造を示す。トランスポートパケットのデータ構造は M P E G システム規格
25 書である I S O / I E C 1 3 8 1 8 - 1 に述べられているので、その説明は省略する。

統合力ボケーションリストはトランスポートパケットの d a t a _

b y t e の部分すなわち、図 1 0 でのペイロードの部分に格納され、ある所定の P I D が割り当てられる。この P I D を仮に R e v o c a t i o n _ p i d とする。実施の形態 1 では統合リボケーションリストは M P E G システム規格のセクション構造に格納する。図 1 2 は統合リボケーションリストをセクション構造に格納した場合のデータ構造の例を示す。統合リボケーションリストのテーブルを仮に R e v o c a t i o n _ l i s t _ t a b l e と称するが、もちろん、他の名前であっても構わない。このデータ構造において、m a k e r _ i d (1 6 ビット) と k i k i _ i d (3 2 ビット) と d e v i c e _ K S V (4 0 ビット) は、S T B から吸い上げたメーカー I D と機器 I D と違反した個々の B k s v である。ただし、メーカー I D 、機器 I D は何ビットであっても構わない。

次に、各 S T B における統合リボケーションリストの受信の方法について説明する。図 1 3 は S T B での統合リボケーションリストの受信フローを示す。

ステップ 2 0 1 において、

S T B が R e v o c a t i o n _ l i s t _ t a b l e を含む T S (トランスポートストリーム) を受信する。

ステップ 2 0 2 において、

S T B の T S デコーダ部 1 1 0 4 で T S から R e v o c a t i o n _ l i s t _ t a b l e を含むパケットを抽出するように、コントロール部 1 1 0 6 は、T S デコーダ部 1 1 0 4 に P I D フィルタに R e v o c a t i o n _ p i d を設定する。P I D フィルタとは、指定した P I D を持ったパケットを抽出するためのもので T S デコーダには必須の機能ある。

ステップ 2 0 3 において、

T S デコーダ部 1 1 0 4 は R e v o c a t i o n _ l i s t _ t a

b 1 e を含むパケットを抽出し、コントロール部 1 1 0 6 が統合リボ
ケーションリストを取得する。

ステップ 2 0 4 において、

5 コントロール部 1 1 0 6 は、取得した統合リボケーションリストを
メモリ部 1 1 0 7 に格納する。

図 1 4 はメモリ部 1 1 0 7 に格納された統合リボケーションリスト
を示す。これにより、すべての S T B で統合リボケーションリストを
共有することが可能になる。

10 そして、新たなディスプレイが S T B に接続された場合に、次のよ
うに動作が実行される。ディスプレイから読み出したメーカー I D、
機器 I D、B k s v が S T B のメモリ部に保持しているリボケーショ
ンリストに同一のものがあれば、初期認証は失敗として、以降そのデ
ィスプレイを使用できなくされる。

15 ところで、以上の説明では、リボケーションリストに含まれる情報
の例として、不正機器として排除すべき機器のメーカー I D と機器 I
D と B k s v が含まれる場合を挙げている。しかし、本発明は、不正
機器として排除すべき機器のメーカー I D と機器 I D と B k s v とが
必ずしも全てリボケーションリストに含まれる必要はない。例えば、
不正機器として排除すべき機器の B k s v のみがリボケーションリス
20 トに含まれる方式でもよい。

図 1 5 から図 1 8 は、不正機器として排除すべき機器の B k s v の
みがリボケーションリストに含まれる場合を説明する為の図である。
図 1 5 は、図 6 において B k s v のみがリボケーションリストに含ま
れる場合に相当する。図 1 6 は、図 8 において B k s v のみがリボケ
25 ーションリストに含まれる場合に相当する。図 1 7 は、図 1 2 におい
て B k s v のみがリボケーションリストに含まれる場合に相当する。
図 1 8 は、図 1 4 において B k s v のみがリボケーションリストに含

まれる場合に相当する。図 1 5 の図 6 に対する相違点と、図 1 6 の図 8 に対する相違点と、図 1 7 の図 1 2 に対する相違点と、図 1 8 の図 1 4 に対する相違点は、不正機器として排除すべき機器の B k s v のみがりボケーションリストに含まれる点である。従って、図 1 5 から
5 図 1 8 の更なる説明は省略する。

りボケーションリストのアップロード～統合りボケーションリスト送出までのフローはそれぞれ、図 7、図 9 において、メーカー I D、機器 I D が含まれていないものとなる。

以上のように実施の形態 1 によれば、S T B とディスプレイの初期
10 認証処理において失敗した場合、その機器を不正機器とし、その機器のメーカー I D と機器 I D と K S V が S T B のメモリ部に格納されてりボケーションリストが作成される。各 S T B からネットワークを通じてりボケーションリストがりボケーションリスト統合部にアップロードされる。りボケーションリスト統合部は、各 S T B よりアップロー
15 ドされたりボケーションリストを統合する。その後、セクションにパッケージ化され、それを T S に多重化され、多重された T S が送信部から送出される。S T B は送信部から送出された T S を受信し、統合りボケーションリストを取得することで、もともと各 S T B で個別に所有するりボケーションリストを、全ての S T B で共有することが可能
20 となる。これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

(実施の形態 2)

次に本発明の実施の形態 2 について説明する。実施の形態 1 と異なるのは統合りボケーションリストのパッケージ化の方法である。図 1 9
25 は実施の形態 2 での統合りボケーションリストを含むパッケージのデータ構造を示す。実施の形態 2 では、図 1 0 に示されている M P E G システム規格の P E S パッケージに統合りボケーションリストを格納する。

図 20 は実施の形態 2 における統合リボケーションリストの受信フローを示す。

ステップ 301 において、

5 STB が統合リボケーションリストの格納された PES パケットを含む TS を受信する。

ステップ 302 において、

10 STB の TS デコーダ部 1104 で TS から統合リボケーションリストを含むパケットを抽出するように、コントロール部 1106 は、TS デコーダ部 1104 の PID フィルタに `Revocation_pid` を設定する。

ステップ 303 において、

TS デコーダ部 1104 は統合リボケーションリストを含むパケットを抽出し、コントロール部 1106 は統合リボケーションリストを取得する。

15 ステップ 304 において、

コントロール部 1106 は取得した統合リボケーションリストを、メモリ部 1107 に格納する。これにより、すべての STB で統合リボケーションリストを共有することが可になる。

20 以上のように実施の形態 2 によれば、STB とディスプレイの初期認証処理において失敗した場合にはその機器は不正機器とし、その機器のメーカー ID、機器 ID、KSV は STB のメモリ部に格納されてリボケーションリストが作成される。そうして、各 STB からのリボケーションリストはネットワークを通じてリボケーションリスト統合部にアップロードされる。リボケーションリスト統合部は各 STB
25 よりアップロードされたりボケーションリストを統合する。その後、リボケーションリストは PES パケットにパケット化され、それが TS に多重化される。送信部は多重化された TS を送出する。STB は

送信部から送出されたTSを受信し、統合リボケーションリストを取得することで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となる。これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

ところで、以上の実施の形態では、リボケーションリストに含まれる情報の例として、不正機器として排除すべき機器のメーカーIDと機器IDとBksvが含まれる場合を挙げている。しかし、本発明は、不正機器として排除すべき機器のメーカーIDと機器IDとBksvとが必ずしも全てリボケーションリストに含まれる必要はない。例えば、不正機器として排除すべき機器のBksvのみがリボケーションリストに含まれる方式でもよい。

また、図21の図19に対する相違点は、不正機器として排除すべき機器のBksvのみがリボケーションリストに含まれている点である。

従って、図21の更なる説明は省略する。

（実施の形態3）

次に本発明の実施の形態3について説明する。実施の形態1と異なるのは統合リボケーションリストの packets 化の方法である。図22は実施の形態3での統合リボケーションリストを含む packets のデータ構造を示す。実施の形態3では、図22に示されるように、MPEGシステム規格のTS packets のペイロードに PES packets やセクション等のデータ構造をとらずにそのまま統合リボケーションリストを格納する。

図23は実施の形態3における統合リボケーションリストの受信フローを示す。

ステップ401において、

STBが統合リボケーションリストの格納された packets を含むT

Sを受信する。

ステップ402において、

5 コントロール部1106は、STBのTSデコーダ部1104でTSから統合リボケーションを含むパケットを抽出するように、TSデコーダ部1104のPIDフィルタにRevocation_pidを設定する。

ステップ403において、

10 TSデコーダ部1104は統合リボケーションリストを含むパケットを抽出し、コントロール部1106は統合リボケーションリストを取得する。

ステップ404において、

 コントロール部1106は取得した統合リボケーションリストを、メモリ部1107に格納する。

15 これにより、すべてのSTBで統合リボケーションリストを共有することが可になる。

 以上のように実施の形態3によれば、STBとディスプレイの初期認証処理において失敗した場合にはその機器を不正機器とし、その機器のメーカーID、機器ID、KSVをSTBのメモリ部に格納してリボケーションリストが作成される。そして、各STBからネットワークを通じてリボケーションリストがリボケーションリスト統合部にアップロードされる。リボケーションリスト統合部は各STBよりアップロードされたりボケーションリストを統合する。その後、TSパケットのペイロードに格納することでパケット化され、それがTSに多重化される。送信部は多重化されたTSを送出する。STBは送信部から送

20 信部から送

25 信部から送

 出されたTSを受信し、統合リボケーションリストを取得する。こうすることで、もともと各STBで個別に所有するリボケーションリストを、全てのSTBで共有することが可能となる。これに

より著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

ところで、既に記載した様に、本発明は、不正機器として排除すべき機器のメーカーIDと機器IDとBk s vとの全てがリポケーションリストに含まれる必要はない。例えば、不正機器として排除すべき機器のBk s vのみがリポケーションリストに含まれる方式でもよい。図24は、不正機器として排除すべき機器のBk s vのみがリポケーションリストに含まれる場合を説明する為の図である。図24の図22に対する相違点は、不正機器として排除すべき機器のBk s vのみがリポケーションリストに含まれる点である。従って、図24の更なる説明は省略する。

(実施の形態4)

次に本発明の実施の形態4について説明する。実施の形態1と異なるのは、デジタル放送ではなくインターネット経由で統合リポケーションリストを各STBに伝送することである。図25は実施の形態4におけるリポケーション情報の送信方法、受信方法を実現するシステムの構成を示す。実施の形態1と異なる部分についてのみ説明する。

STB#1' 201~STB#N' 203はインターネットへのインタフェースを有するSTBである。

図26はSTB#1' 201~STB#N' 203の内部構成を示す。図3に示された実施の形態1のSTBと異なる部分についてのみ説明する。LAN I/F2001は後述するネットワークに接続され、IPパケットをやり取りするインタフェースである。

ネットワーク204~207はインターネットによるネットワークである。送出センター208は、統合リポケーションリストをIPパケットに格納する。送信部209は統合リポケーション情報が格納されたIPパケットを送出する。

以上のように構成された実施の形態 4 についてその動作を説明する。
実施の形態 1 と異なるものについて説明する。

実施の形態 4 では、S T B # 1 ' 2 0 1 ~ S T B # N ' 2 0 3 がリ
ボケーションリストを作成するまでは実施の形態 1 と同一である。図
5 2 7 はリボケーションリストのアップロード～送出までのフローを示
す。

ステップ 5 0 1 において、

S T B のコントロール部 1 1 0 6 が、メモリ部 1 1 0 7 に格納され
たりボケーションリストからメーカー I D、機器 I D、B k s v を読
10 み出し、L A N I / F 2 0 0 1 に転送する。

ステップ 5 0 2 において

S T B の L A N I / F 2 0 0 1 からネットワーク 2 0 4、ネット
ワーク 2 0 5、ネットワーク 2 0 6 経由で B k s v がリボケーション
リスト統合部 1 1 4 にアップロードされる。

15 ステップ 5 0 3 において、

リボケーションリスト統合部 1 1 4 は、所定期間に各 S T B からア
ップロードされた B k s v の一覧を作成し、これを統合リボケーショ
ンリストとする。

ステップ 5 0 4 において、

20 リボケーションリスト統合部 1 1 4 から送出センター 2 0 8 に統合
リボケーションリストが伝送される。

ステップ 5 0 5 において、

送出センター 2 0 8 は、統合リボケーションリストを I P パケット
に格納する。

25 ステップ 5 0 6 において、

送信部 2 0 9 は、統合リボケーションリストが格納された I P パケ
ットを各 S T B に送信する。

ここで、ステップ 505 での統合リボケーションリストのパケット化について説明する。図 28 は IP パケットのデータ構造の一例を模式的に示す。このパケットのデータの部分に実施の形態 1 と同様な統合リボケーション情報が格納される。

- 5 次に、各 STB における統合リボケーションリストの受信の方法について説明する。図 29 は STB での統合リボケーションリストの受信フローを示す。

ステップ 601 において、

- 10 STB が LAN I/F 2001 で統合リボケーションリストを含む IP パケットを受信する。

ステップ 602 において、

STB のコントロール部 1106 が LAN I/F 2001 からの統合リボケーションリストを抽出し、取得する。

ステップ 603 において、

- 15 コントロール部 1106 は、取得した統合リボケーションリストをメモリ部 1107 に格納する。

これにより、すべての STB で統合リボケーションリストを共有することが可能になる。

- 20 そして、新たなディスプレイが STB に接続された場合に、ディスプレイから読み出したメーカー ID、機器 ID、B k s v が STB のメモリ部に保持しているリボケーションリストに同一のものがあるか否か確認される。同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくされる。

- 25 以上のように実施の形態 4 によれば、STB とディスプレイの初期認証処理において失敗した場合には、その機器を不正機器とし、その機器のメーカー ID、機器 ID、K S V を STB のメモリ部に格納してリボケーションリストを作成する。各 STB からネットワークを通

じてリボケーションリストをリボケーションリスト統合部にアップロードする。リボケーションリスト統合部は各S T Bよりアップロードされたりボケーションリストを統合する。その後、I P パケットにパケット化されて、送信部から送出される。S T Bは送信部から送出されたI P パケットを受信し、統合リボケーションリストを取得すること
5 5 ことで、もともと各S T Bで個別に所有するリボケーションリストを、全てのS T Bで共有することが可能となる。これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

ところで、以上の実施の形態では、リボケーションリストに含まれる情報の例として、不正機器として排除すべき機器のメーカーI Dと機器I DとB k s vが含まれる場合を挙げている。しかし、本発明は、不正機器として排除すべき機器のメーカーI Dと機器I DとB k s v
10 10 とが必ずしも全てリボケーションリストに含まれる必要はない。例えば、不正機器として排除すべき機器のB k s vのみがリボケーションリストに含まれる方式でもよい。

(実施の形態5)

次に本発明の実施の形態5について説明する。図30は実施の形態5におけるリボケーション情報の送信方法、受信方法を実現するシステム
20 20 の構成を示す。実施の形態1と異なるのは、リボケーションリストをS T Bからアップロードするのではなく、リボケーションリスト統合部301で統合リボケーションリストを発行するという点である。リボケーションリストは、初期認証が失敗の場合、ユーザがリボケーションリストを管理している機関に、不正機器の疑いがあることを直接
25 25 的、あるいは間接的に連絡をする。これに応じて、リボケーションリスト管理機関は、不正機器の疑いのある機器を回収する。あるいは、リボケーションリスト管理機関は、不正機器の疑いのある機器のリボ

ケーション情報を入手する。ここでリボケーション情報は、不正機器の Bksv を含む。リボケーション管理機関は、入手したリボケーション情報を用いて、リボケーション情報を含む統合リボケーションリストを作成する。統合リボケーションリストは実施の形態 1 ～ 3 のように
5 TS に多重化してもよいし、実施の形態 4 のように IP パケットに格納してもよい。総合リボケーションリストを作成したあとの処理は実施の形態 1 ～ 4 と同一である。

以上のように本実施の形態 5 によれば、STB からリボケーションリストをアップロードすることなく、リボケーションリスト統合部で
10 統合リボケーションリストを作成される。送出センター 115 は作成された統合リボケーションリストを TS や IP パケットに格納し、送信部 116 はそれを送出する。STB は送信部 116 から送出された TS を受信し、統合リボケーションリストを取得することで、もともと各 STB で個別に所有するリボケーションリストを、全ての STB
15 で共有することが可能となる。これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

ところで、以上の説明では、初期認証の処理が失敗の場合、ユーザがリボケーションリストを管理している機関にそのリボケーションリストを連絡する場合を例に挙げている。しかし、本発明は、ユーザが
20 リボケーション機器の情報を連絡する方式に限られるものではない。即ち、ある特定の機関がリボケーションリストを管理している機関にそのリボケーション機器の情報を連絡する方式であっても良い。またリボケーションリストを管理している機関が、リボケーション機器情報を調査する方式であってもかまわない。

25 なお、以上の各実施の形態では STB をコンテンツ送出機器の例として説明したが、コンテンツ送出機器は DVD プレーヤや DVD レコーダや PC など他の機器であっても構わない。またデジタルインタフ

エースとして、HDMIを例にとって説明したがDVIやIEEE 1394であっても構わない。また、以上の各実施の形態ではディスプレイをコンテンツ受信機器の例として説明したが、コンテンツ受信機器はディスプレイに限られるものではない。

5 また、ディスプレイはAVスイッチャーなどのリピーター機器であっても構わない。また、統合リボケーションリストはTSパケットやIPパケット以外のものに格納して伝送しても構わない。またリボケーションリストをアップロードするための手段は、電話やインターネット以外のネットワークであっても構わない。

10 また、以上の各実施の形態においては、配信された統合リボケーションリストと機器とを照合して著作権保護上不正な機器であるか否かを判断している。本発明では、配信された統合リボケーションリストと機器とを照合した結果、著作権保護上不正な機器であることが判明した場合に、コンテンツを送出する側の機器から映像信号や音声信号
15 を出力しないことも可能である。こうすることで、著作権保護上不正な機器へのコンテンツ流出が更に防ぐことができる。

また、以上の実施の形態1～実施の形態3の説明では、統合リボケーションリストをMP EGシステム規格のTSパケットにどのような形式で格納するかについて記載している。本発明での統合リボケーションリストのTSパケットへの格納形式は、上述の形式に限られるものではない。即ち、統合リボケーションリストはMP EGシステム規格のTSに多重可能な部分であれば、どこに多重しても構わない。例えば、アダプテーションフィールド（adaptation__field）やプライベートセクション（private__section）や、セクション構造の格納可能なdescriptorやPESパケットの
20 前述した部分以外の部分に統合リボケーションリストを多重しても構わない。

以上のようにこの発明によれば、著作権保護上、不正なディスプレイのリボケーションリストをS T B等の全ての映像出力機器で共有することで、不正なディスプレイを排除することが可能となる。そして、映像出力機器とディスプレイとを接続するデジタルインタフェースの
5 セキュリティを向上させるという効果を有する。

産業上の利用可能性

発明によるリボケーション情報の送信方法、リボケーション情報の受信方法、リボケーション情報の送信装置、及びリボケーション情報の
10 の受信装置は、リボケーションリストをS T B等の全ての映像出力機器に共有させることができ、不正なディスプレイを排除することが可能である。そして、映像出力機器とディスプレイとを接続するデジタルインタフェースのセキュリティを向上させるという効果を有する。

請求の範囲

1. コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、
5 前記コンテンツ送出機器と前記コンテンツ受信機器が相互認証を行なうステップと、
前記相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーション情報をアップロードするステップと、
10 アップロードされた個々の前記リボケーション情報を統合して統合リボケーション情報を作成するステップと、
前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、
15 前記ストリームを送出するステップと
を備えるリボケーション情報の送信方法。
2. 1個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合して統合リボケーション情報を作成するステップと、
20 前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、
前記ストリームを送出するステップと
を備えるリボケーション情報の送信方法。
- 25 3. 前記ストリームはMPEGトランスポートストリームであり、前記統合リボケーション情報は前記MPEGトランスポートストリー

ムのセクションのデータ構造を用いて伝送される請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

4. 前記ストリームは M P E G トランスポートストリームであり、

- 5 前記統合リボケーション情報は前記 M P E G トランスポートストリームの P E S パケットのデータ構造を用いて伝送される請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

5. 前記ストリームは M P E G トランスポートストリームであり、

- 10 前記統合リボケーション情報は M P E G トランスポートストリームのトランスポートパケットのペイロードを用いて伝送される請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

6. 前記統合リボケーション情報は I P パケットを用いて伝送される

- 15 請求項 1 または請求項 2 に記載のリボケーション情報の送信方法。

7. コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信するステップと、

前記コンテンツ送出機器または前記コンテンツ受信機器が前記

- 20 統合リボケーションリストを記憶するステップと
を備えるリボケーション情報の受信方法。

8. 前記統合リボケーションリストと前記コンテンツ受信機器から読み出したキー情報の照合処理ステップと、

- 25 前記キー情報がリボケーションリストにあれば、認証を失敗として、前記コンテンツ受信機器から映像または音声出力を阻止するステップと

をさらに備える請求項 7 記載のリボケーション情報の受信方法。

9. コンテンツを送出する複数のコンテンツ送出機器と、

前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、

前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段と、

前記複数のコンテンツ送出機器または前記複数の受信機器からリボケーション情報を吸い上げるネットワークと

前記ネットワークに接続され、前記リボケーション情報を統合する統合手段と、

前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、

前記ストリームを送信する送信手段と

を備えるリボケーション情報の送信装置。

10. 1 個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合する統合手段と、

前記統合リボケーション情報をパケット化してストリームに多

重する多重化手段と、

前記ストリームを送信する送信手段と

を備えるリボケーション情報の送信装置。

11. 前記ストリームは M P E G トランスポートストリームであり、

前記統合リボケーション情報は前記 M P E G トランスポートストリームのセクションのデータ構造を用いて伝送される請求項 9 または請求項 10 に記載のリボケーション情報の送信装置。

12. 前記ストリームはMPEGトランスポートストリームであり、
前記統合リボケーション情報は前記MPEGトランスポートストリー
ムのPESパケットのデータ構造を用いて伝送される請求項9または
5 請求項10に記載のリボケーション情報の送信装置

10

13. 前記統合リボケーション情報はMPEGトランスポートストリー
ムのトランスポートパケットのペイロードを用いて伝送される請求
項9または請求項10に記載のリボケーション情報の送信装置。

14. 前記統合リボケーション情報はIPパケット用いて伝送される
請求項9または請求項10に記載のリボケーション情報の送信装置。

15. 統合リボケーションリストを受信するコンテンツ送出機器また
15 はコンテンツ受信機器を備え、

前記コンテンツ送出機器または前記コンテンツ受信機器は前記
統合リボケーションリストを記憶するリボケーション情報の受信装置。

16. 前記統合リボケーションリストと前記コンテンツ受信機器から
20 読み出したキー情報の照合処理手段と、

前記キー情報がリボケーションリストにあれば、認証を失敗と
して、前記コンテンツ受信機器から映像または音声を出力を阻止する
出力制御手段と

をさらに備える請求項15記載のリボケーション情報の受信装置。

25

補正書の請求の範囲

[2004年8月30日(30.08.2004)国際事務局受理:出願当初の請求の範囲2,7,8,10,15及び16は取り下げられた;出願当初の請求の範囲1,3,4,5,6,9,11,12,13及び14は補正された;新しい請求の範囲17及び18が加えられた。(5頁)]

1.(補正後) コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ送出機器から前記コンテンツ受信機器に対して圧縮伸張されたデジタル信号を出力する第1のデジタルインターフェースと、前記コンテンツ送出機器と前記コンテンツ受信機器との間でデータの送受信を行う第2のデジタルインターフェース、から構成されるシステムにおいて、前記コンテンツ送出機器が前記コンテンツ受信機器の認証情報を前記第2のデジタルインターフェースを介して読み出して、前記コンテンツ送出機器と前記コンテンツ受信機器との間で相互認証を行なうステップと、

前記相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーション情報をアップロードするステップと、

アップロードされた個々の前記リボケーション情報を統合して統合リボケーション情報を作成するステップと、

前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、

前記ストリームを送出するステップとを備えるリボケーション情報の送信方法。

2.(削除)

3.(補正後) 前記ストリームはMPEGトランスポートストリームであり、前記統合リボケーション情報は前記MPEGトランスポートストリームのセクションのデータ構造を用いて伝送される請求項1

補正された用紙(条約第19条)

に記載のリボケーション情報の送信方法。

4. (補正後) 前記ストリームはMPEGトランスポートストリーム
であり、前記統合リボケーション情報は前記MPEGトランスポート
5 ストリームのPESパケットのデータ構造を用いて伝送される請求項
1に記載のリボケーション情報の送信方法。

5. (補正後) 前記ストリームはMPEGトランスポートストリーム
であり、前記統合リボケーション情報はMPEGトランスポートスト
10 リームのトランスポートパケットのペイロードを用いて伝送される請
求項1に記載のリボケーション情報の送信方法。

6. (補正後) 前記統合リボケーション情報はIPパケットを用いて伝
送される請求項1に記載のリボケーション情報の送信方法。

15

7. (削除)

8. (削除)

20

25

9. (補正後) コンテンツを送出する複数のコンテンツ送出機器と、
前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受
信する複数のコンテンツ受信機器と、前記コンテンツ送出機器から前
記コンテンツ受信機器に対して圧縮伸張されたデジタル信号を出力す
る第1のデジタルインターフェースと、前記コンテンツ送出機器と前
記コンテンツ受信機器との間で前記コンテンツ受信機器の認証情報の
送受信を行う第2のデジタルインターフェースと、

前記複数のコンテンツ送出機器または前記複数の受信機器から
リボケーション情報を吸い上げるネットワークと

10 前記ネットワークに接続され、前記リボケーション情報を統
合する統合手段と、

前記統合手段において統合された統合リボケーション情報を
パケット化してストリームに多重する多重化手段と、

15 前記ストリームを送信する送信手段と
を備えるリボケーション情報の送信装置。

10. (削除)

11. (補正後) 前記ストリームはMPEGトランスポートストリーム
20 であり、前記統合リボケーション情報は前記MPEGトランスポート
ストリームのセクションのデータ構造を用いて伝送される請求項9に
記載のリボケーション情報の送信装置。

12. (補正後) 前記ストリームはMPEGトランスポートストリームであり、前記統合リボケーション情報は前記MPEGトランスポートストリームのPESパケットのデータ構造を用いて伝送される請求項9に記載のリボケーション情報の送信装置

5

13. (補正後) 前記統合リボケーション情報はMPEGトランスポートストリームのトランスポートパケットのペイロードを用いて伝送される請求項9に記載のリボケーション情報の送信装置。

10 14. (補正後) 前記統合リボケーション情報はIPパケット用いて伝送される請求項9に記載のリボケーション情報の送信装置。

15. (削除)

15 16. (削除)

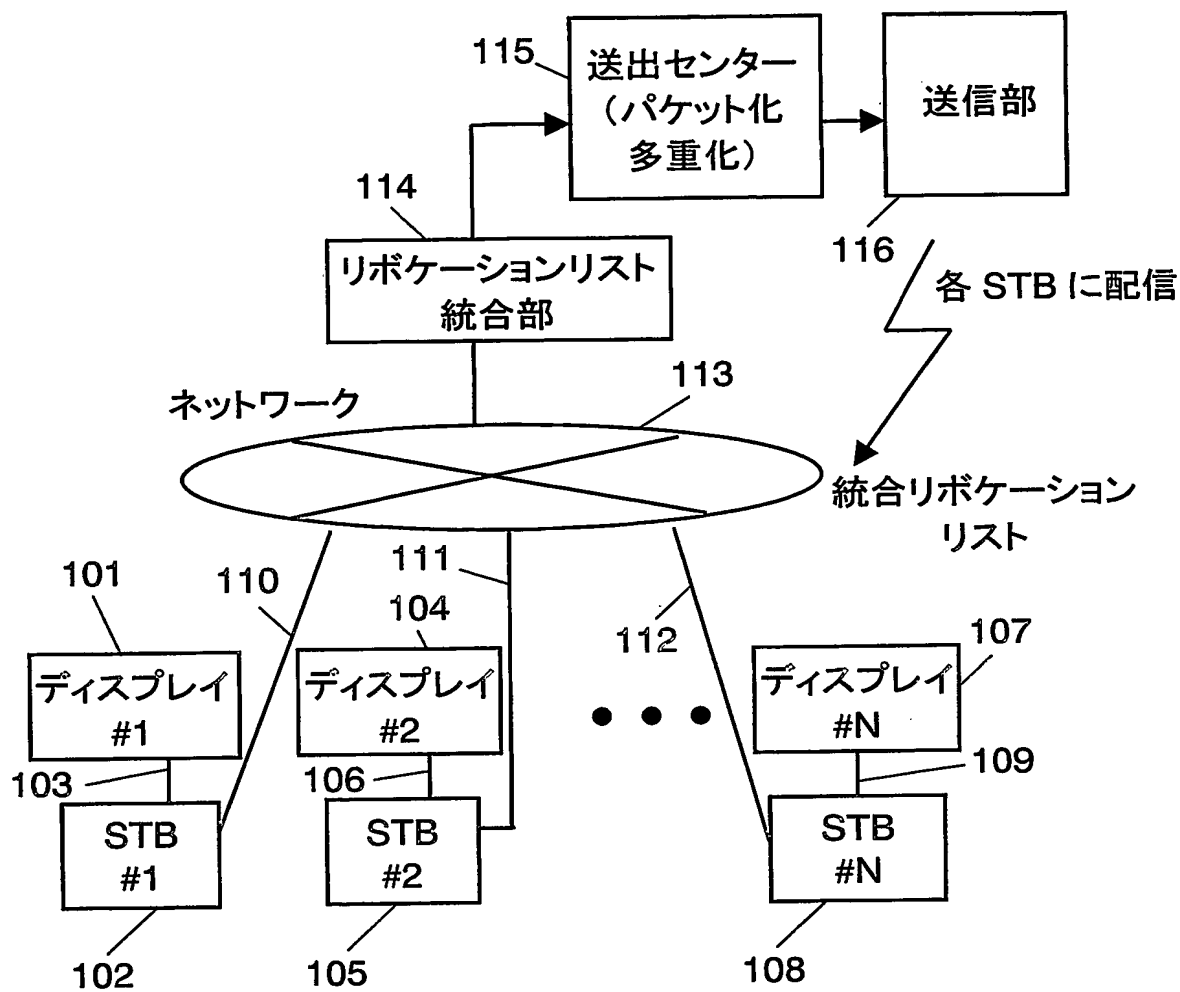
17. (追加) コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ送出機器から前記コンテンツ受信機器に対して圧縮伸張されたデジタル信号を出力する第1のデジタルインターフェースと、前記コンテンツ送出機器と前記コンテンツ受信機器との間でデータの送受信を行う第2のデジタルインターフェース、から構成されるシステムにおいて、
前記コンテンツ送出機器が前記コンテンツ受信機器の認証情報を前記第2のデジタルインターフェースを介して読み出して、前記コンテンツ送出機器と前記コンテンツ受信機器との間で相互認証を行なうステップと、
前記相互認証が失敗の場合、前記コンテンツ送出機器または前記コン

テンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーション情報を出力するステップ
を備えるリボケーション情報の送信方法。

- 5 18. (追加) コンテンツを送出する複数のコンテンツ送出機器と、
前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受
信する複数のコンテンツ受信機器と、前記コンテンツ送出機器から前
記コンテンツ受信機器に対して圧縮伸張されたデジタル信号を出力す
る第1のデジタルインターフェースと、前記コンテンツ送出機器と前
10 記コンテンツ受信機器との間で前記コンテンツ受信機器の認証情報の
送受信を行う第2のデジタルインターフェースと、
前記コンテンツ送出機器と前記コンテンツ受信機器との間で相互認証
を行なう手段と、
前記相互認証が失敗の場合、前記コンテンツ送出機器または前記コン
15 テンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーショ
ン情報を出力する出力手段と
を備えるリボケーション情報の送信装置。

1/19

FIG. 1



2/19

FIG. 2

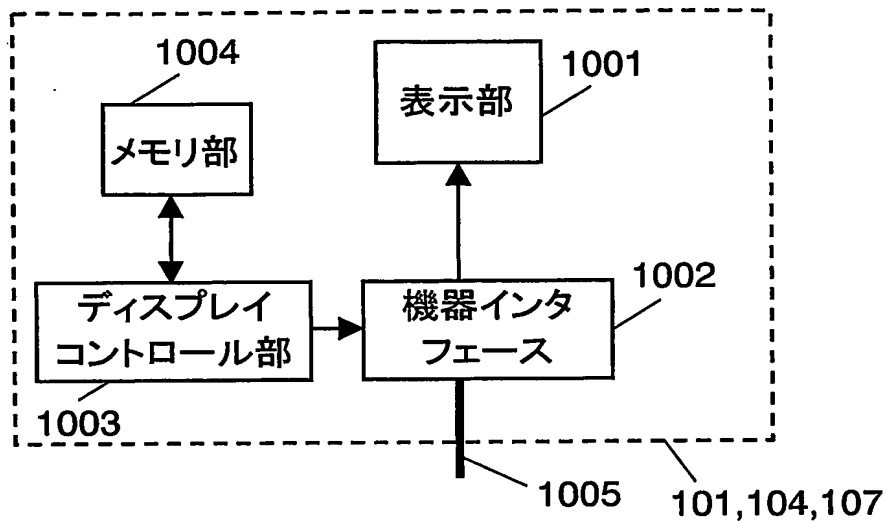
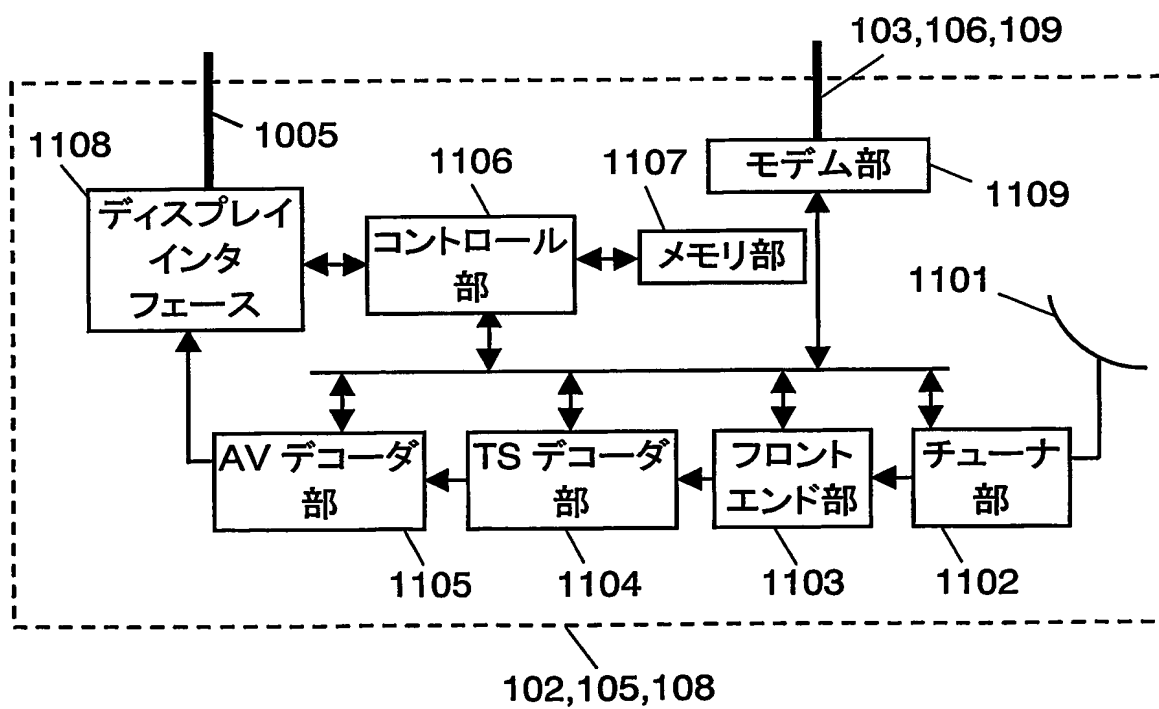


FIG. 3



3/19

FIG. 4

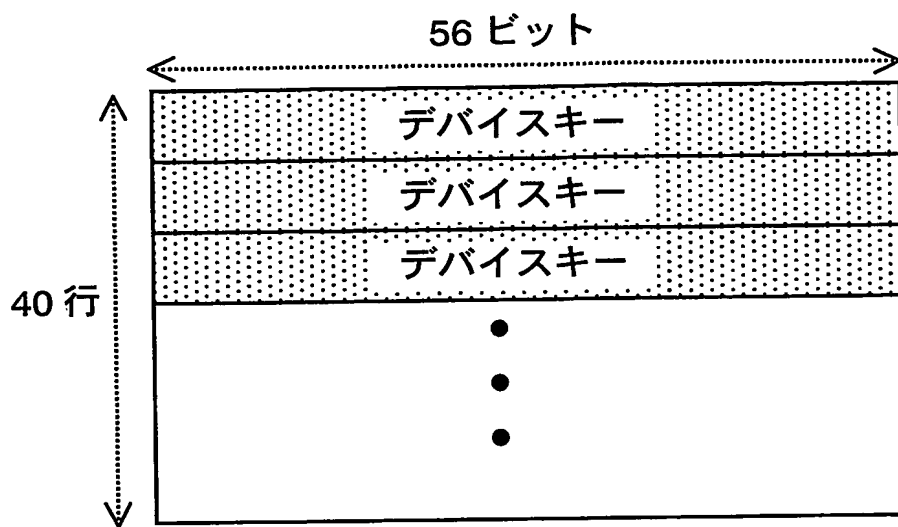
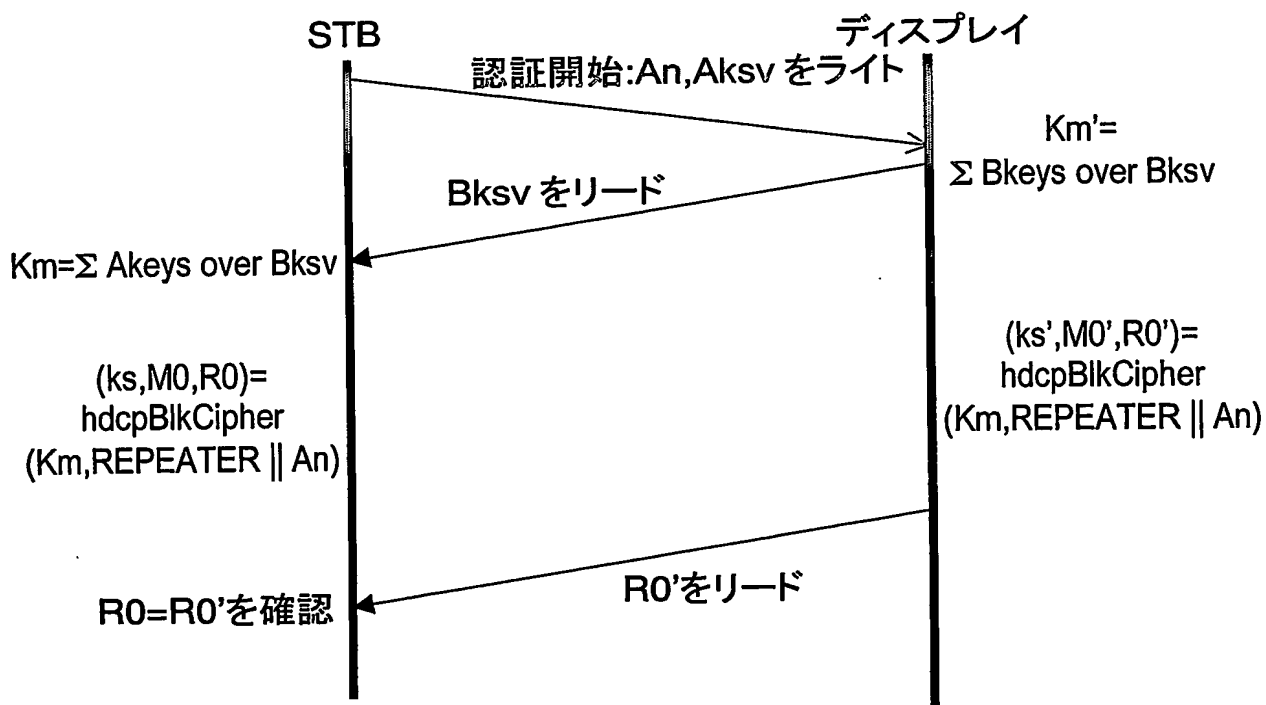


FIG. 5



4/19

FIG. 6

メーカーID	機器 ID	Bksv
Maker_1	Kiki_1	Bksv_1
Maker_2	Kiki_2	Bksv_2
無登録	無登録	無登録
無登録	無登録	無登録

FIG. 7

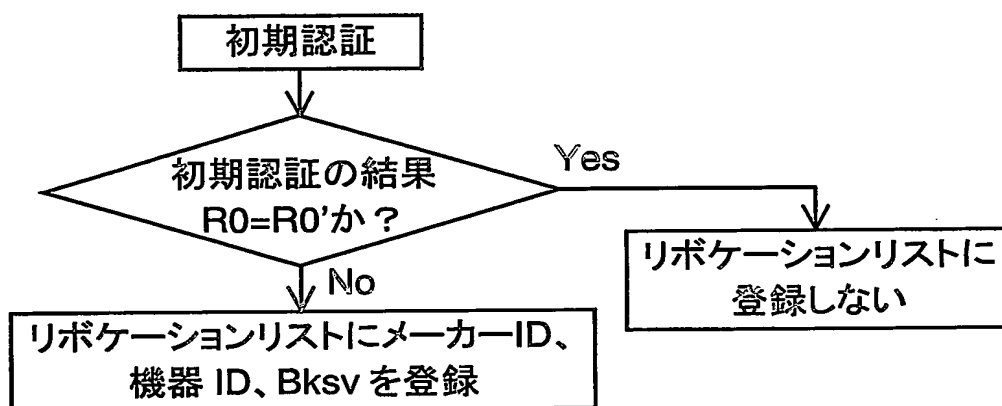


FIG. 8

メーカーID	機器 ID	Bksv
Maker_1	Kiki_1	Bksv_1
Maker_2	Kiki_2	Bksv_2
Maker_3	Kiki_3	Bksv_3
無登録	無登録	無登録

5/19

FIG. 9

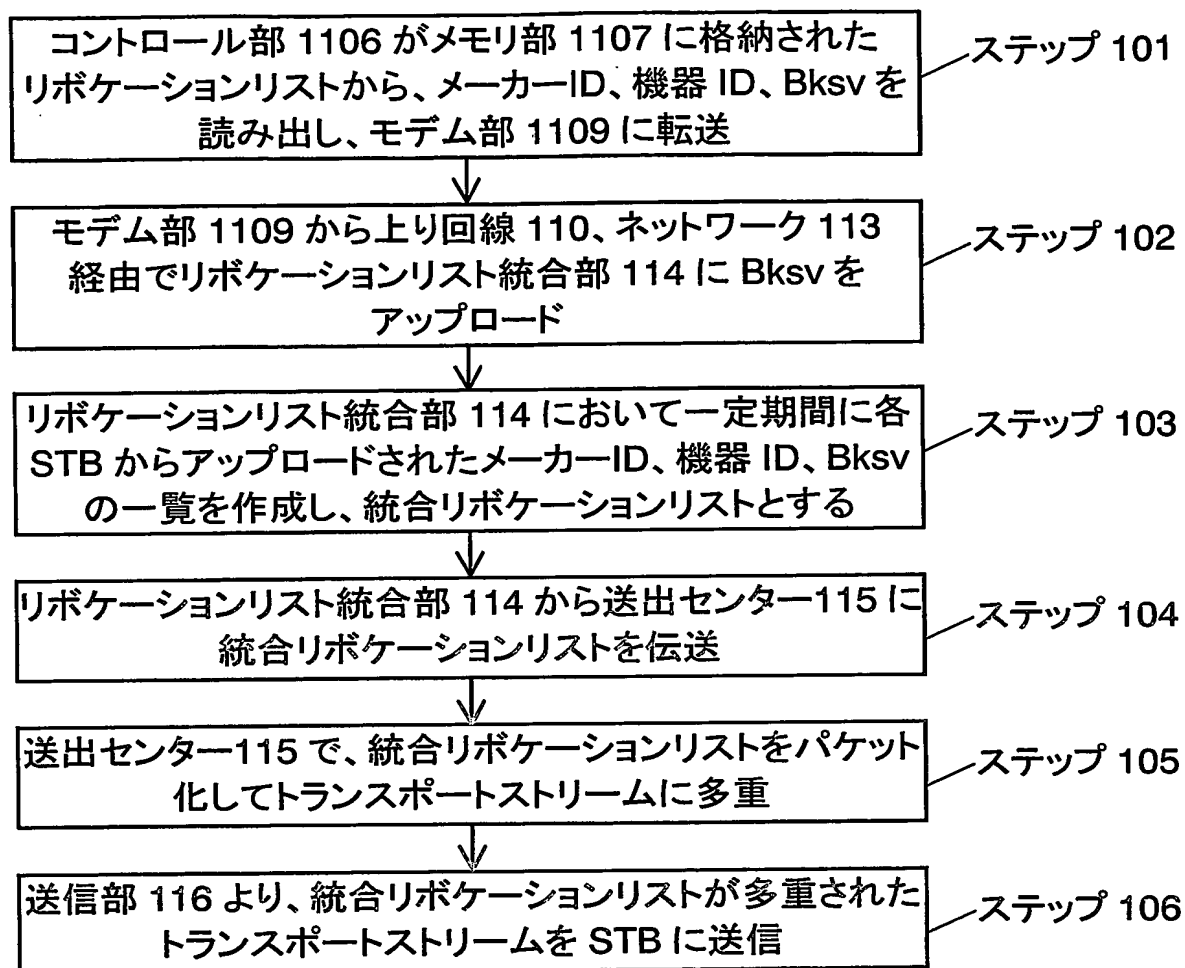
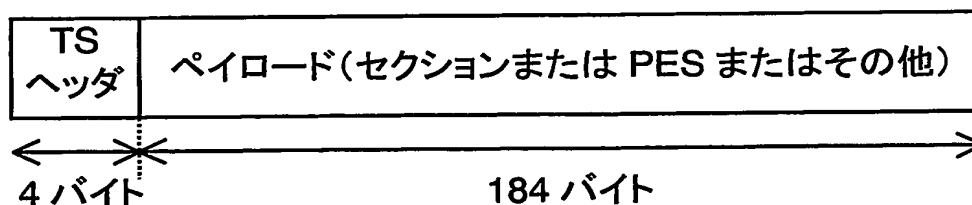


FIG. 10



6/19

FIG. 11

フィールド	ビット数
sync_byte	8
transport_stream_indicator	1
payload_unit_start_indicator	1
transport_priority	1
PID	13
transport_scrambling_control	2
adaptation_field_control	2
continuity_counter	4
for (i=0; i < n; i++){	
data_byte	8
}	

FIG. 12

フィールド	ビット数
table_id	8
section_syntax_indicator	1
reserved	2
section_length	12
program_number	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
for (i=0; i < n; i++){	
marker_id	16
kiki_id	32
device_KSV	40
}	
CRC_32	32

FIG. 13

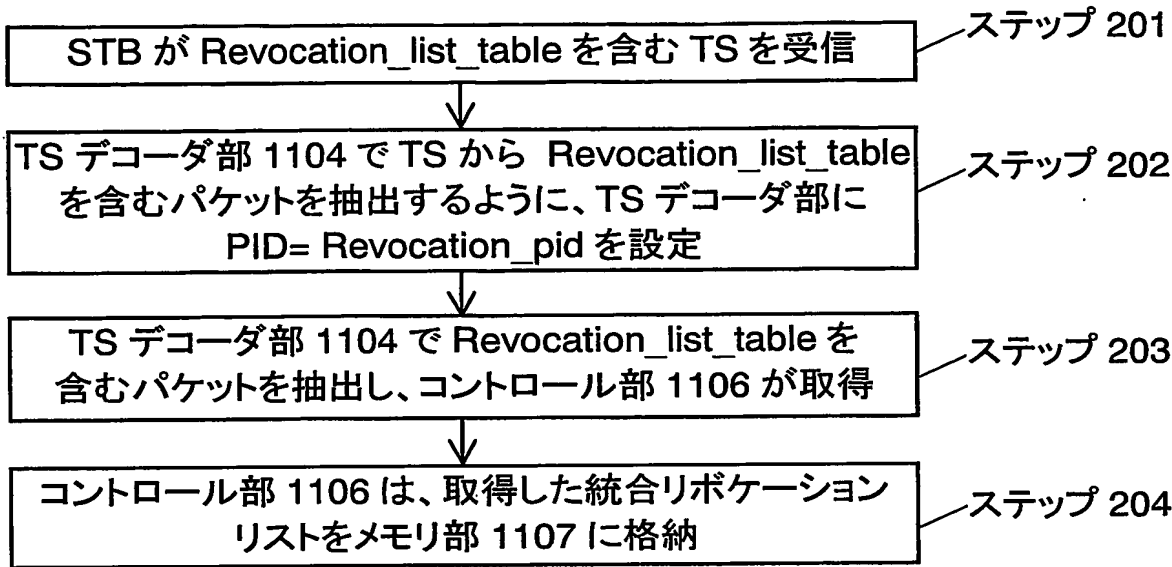


FIG. 14

メーカーID	機器 ID	Bksv
Maker_1	Kiki_1	Bksv_1
Maker_2	Kiki_2	Bksv_2
Maker_3	Kiki_3	Bksv_3
Maker_4	Kiki_4	Bksv_4
Maker_5	Kiki_5	Bksv_5
無登録	無登録	無登録
無登録	無登録	無登録

FIG. 15

Bksv
Bksv_1
Bksv_2
無登録
無登録

FIG. 16

Bksv
Bksv_1
Bksv_2
Bksv_3
無登録

FIG. 17

フィールド	ビット数
table_id	8
section_syntax_indicator	1
reserved	2
section_length	12
program_number	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
for (i=0; i <n;i++){ device_KSV	40
}	
CRC_32	32

9/19

FIG. 18

Bksv
Bksv_1
Bksv_2
Bksv_3
Bksv_4
Bksv_5
無登録
無登録

FIG. 19

フィールド	ビット数
packet_start_code_prefix	24
strem_id	8
PES_packet_length	16
for (i=0;i <PES_packet_length/5;i++){	
maker_id	16
kiki_id	32
device_KSV	40
}	

10/19

FIG. 20

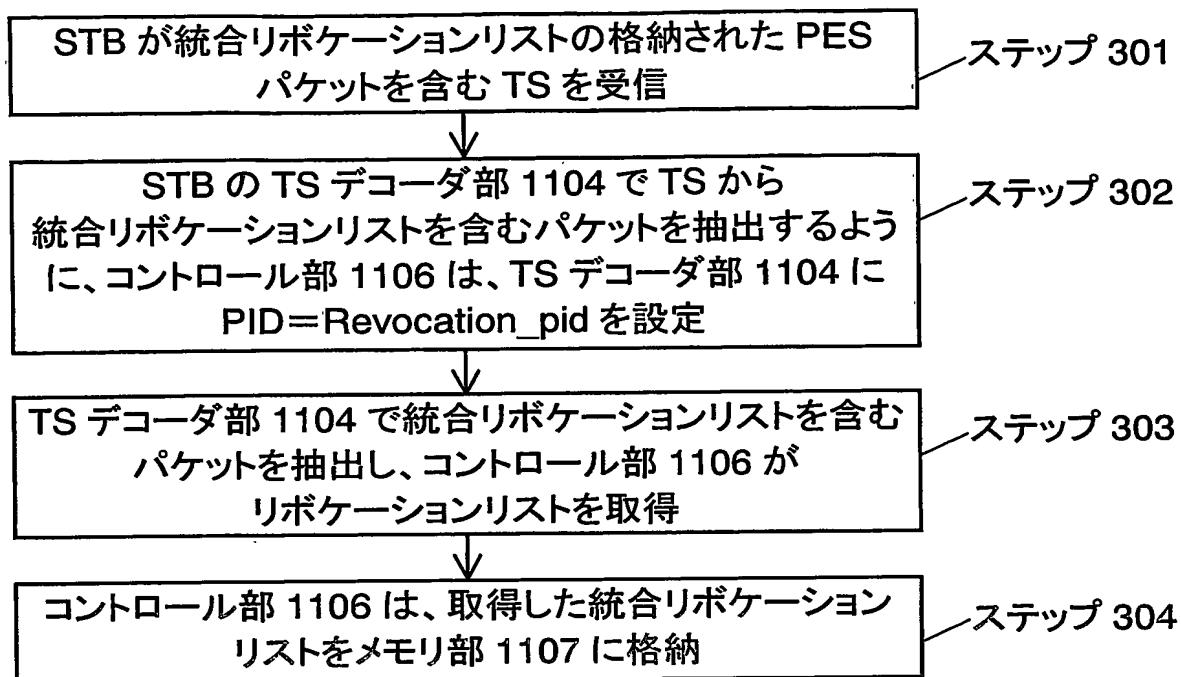


FIG. 21

フィールド	ビット数
packet_start_code_prefix	24
stream_id	8
PES_packet_length	16
for (i=0; i < PES_packet_length/5; i++){ device_KSV	40
}	

FIG. 22

フィールド	ビット数
KSV_number	16
For (l=0; l < KSV_number, l++){ maker_id	16
kiki_id	32
device_KSV	40
}	

11/19

FIG. 23

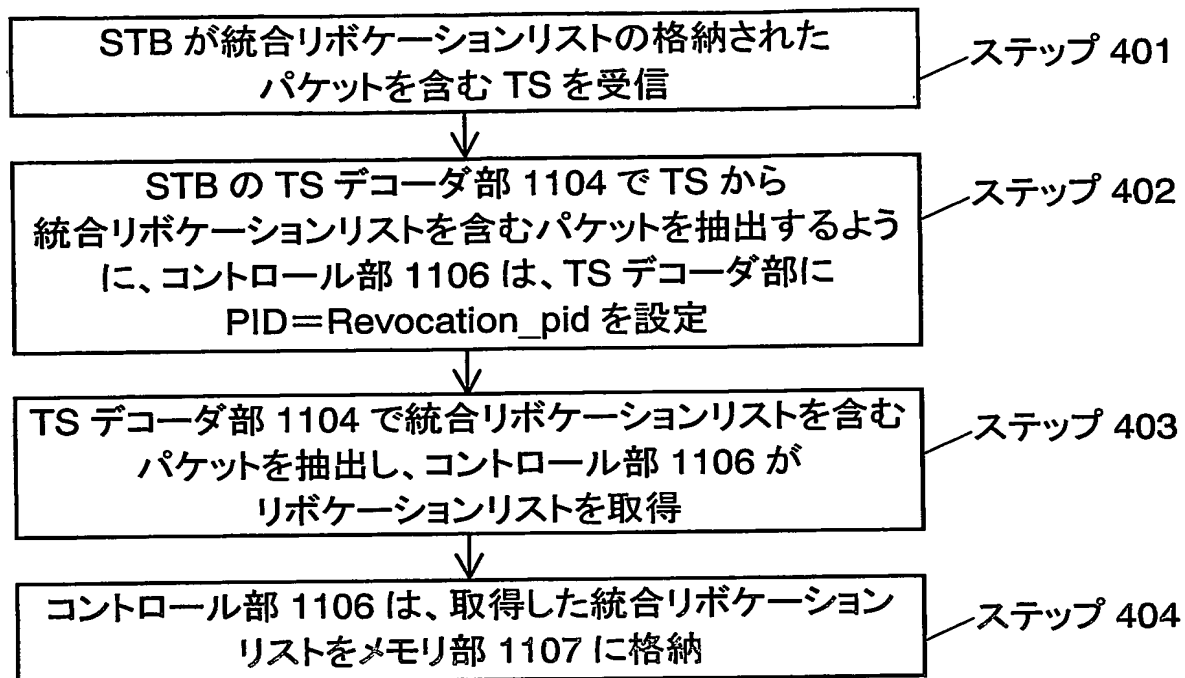
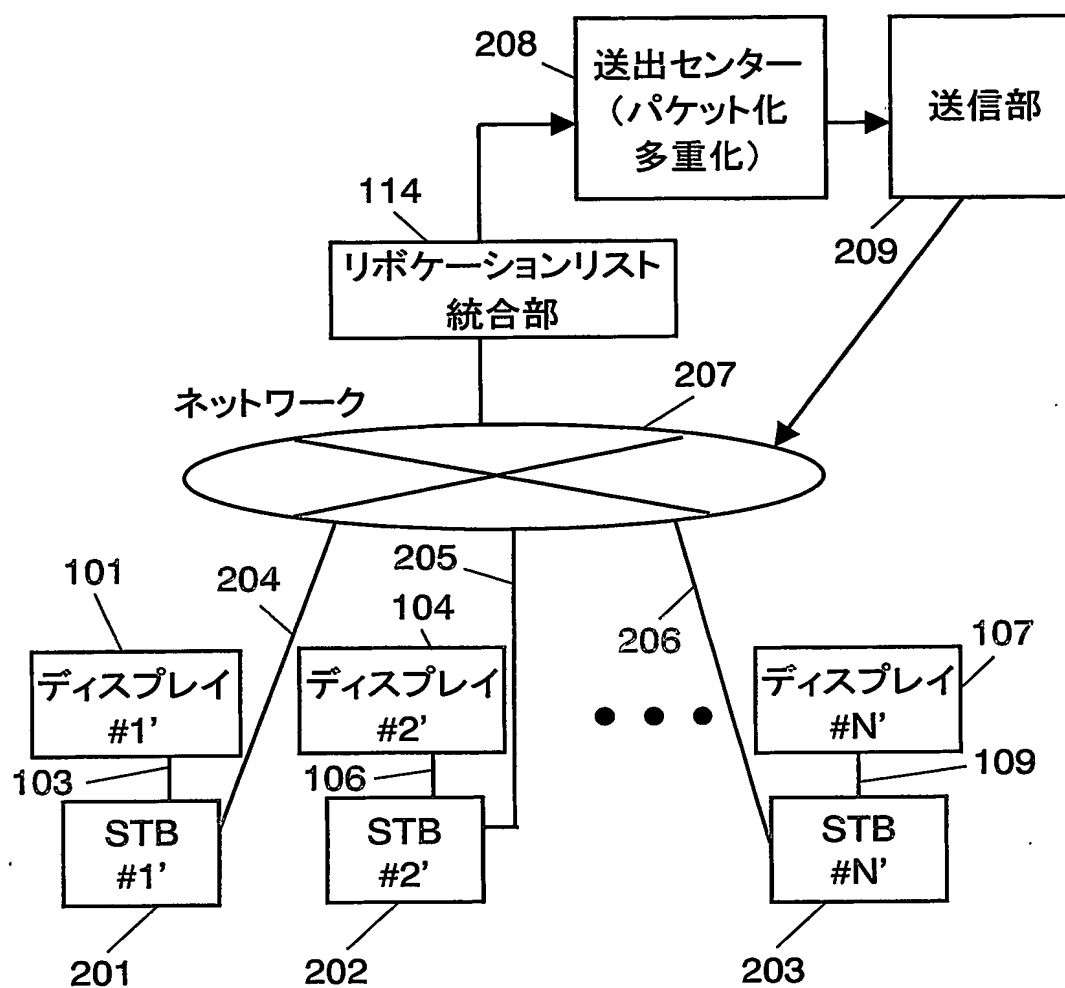


FIG. 24

フィールド	ビット数
KSV_number	16
For (l=0;l <KSV_number,l++){	
device_KSV	40
}	

12/19

FIG. 25



13/19

FIG. 26

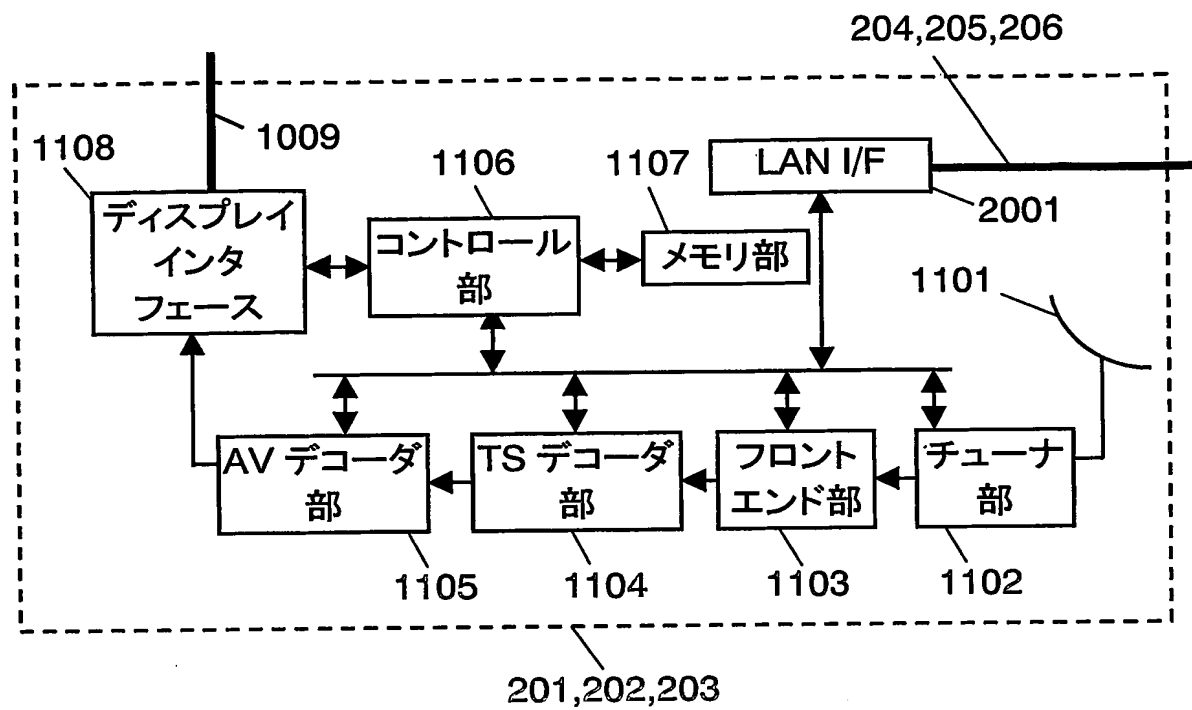


FIG. 27

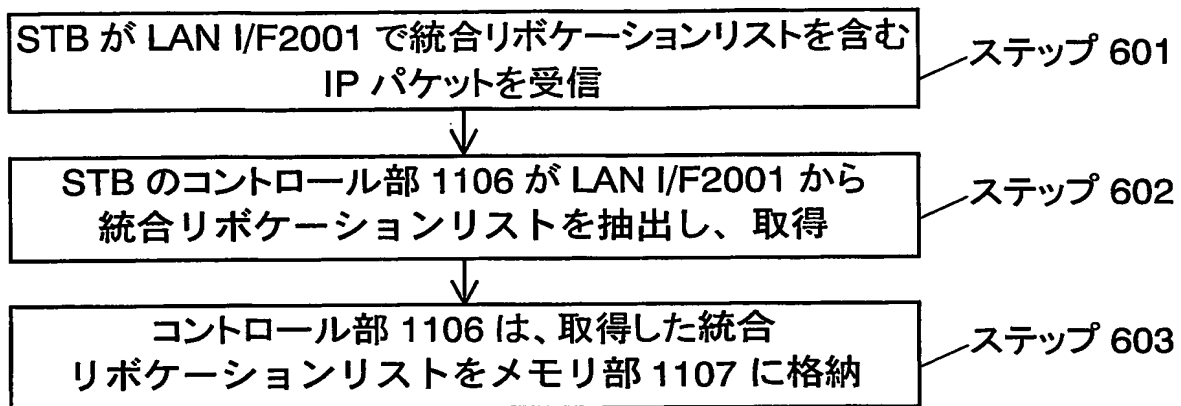


FIG. 28

送信元 IP アドレス	送信先 IP アドレス	プロトコル タイプ	送信元 ポート 番号	送信先 ポート 番号	データ	FCS
-------------------	-------------------	--------------	------------------	------------------	-----	-----

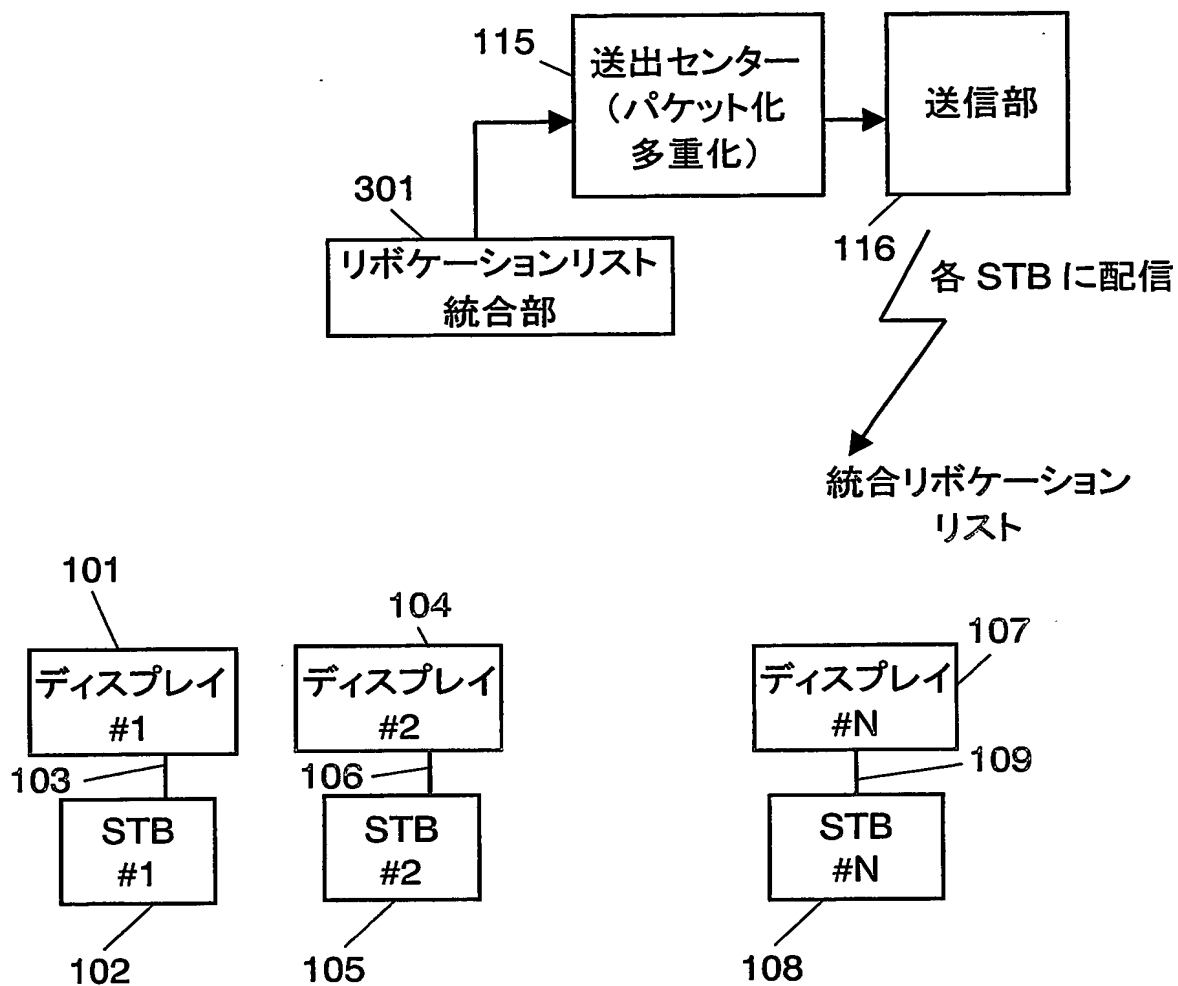
15/19

FIG. 29



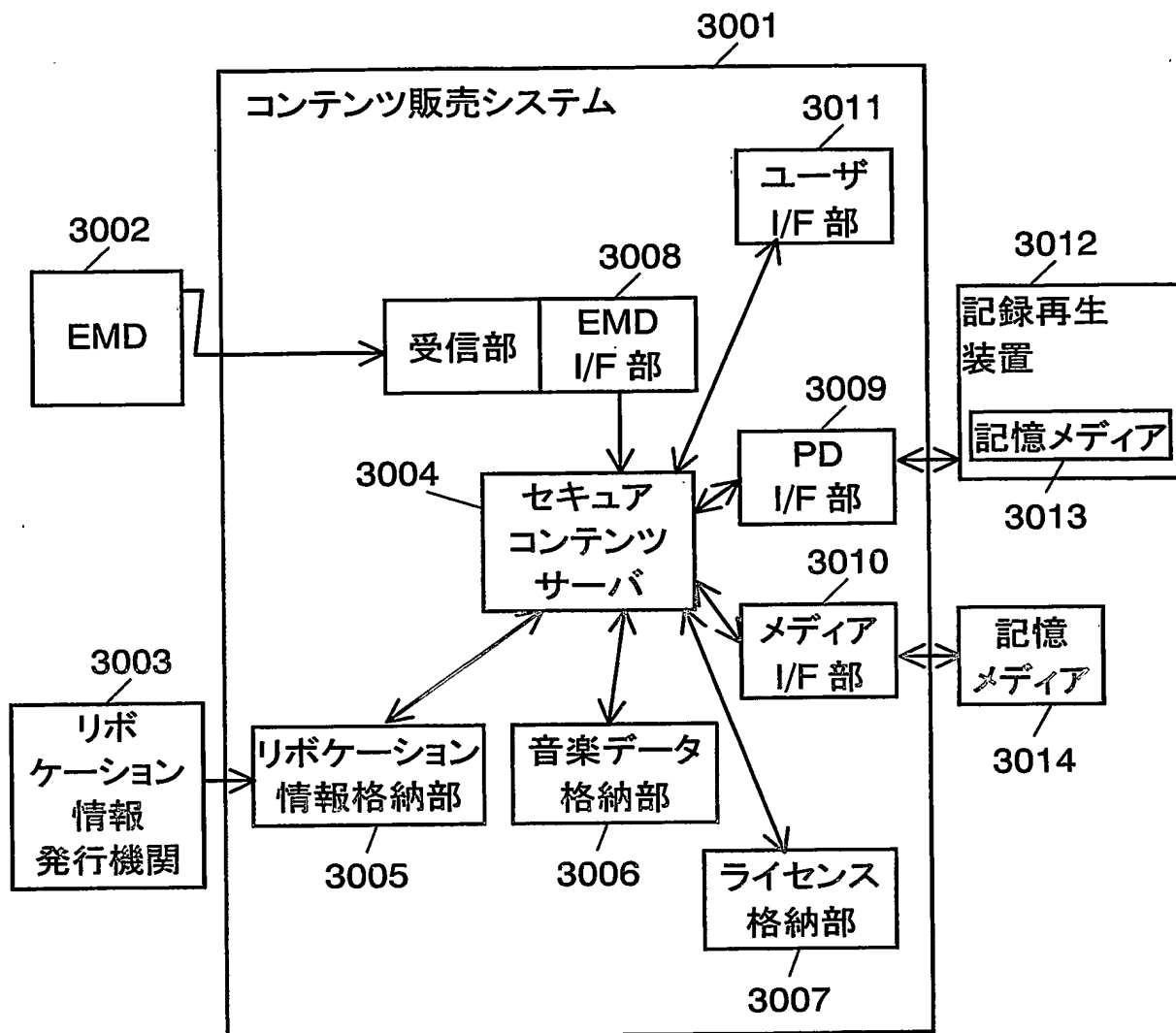
16/19

FIG. 30



17/19

FIG. 31



図面の参照符号の一覧表

- 101 第1のディスプレイ
- 102 第1のSTB
- 103 第1のデジタルインタフェース
- 104 第2のディスプレイ
- 105 第2のSTB
- 106 第2のデジタルインタフェース
- 107 第Nのディスプレイ
- 108 第NのSTB
- 109 第Nのデジタルインタフェース
- 110 第1の上り回線
- 111 第2の上り回線
- 112 第Nの上り回線
- 113 ネットワーク
- 114 リボケーションリスト統合部
- 115 送出センター
- 116 送信部
- 1001 表示部
- 1002 機器インタフェース
- 1003 コントロール部
- 1004 メモリ部
- 1101 アンテナ
- 1102 チューナ部
- 1103 フロントエンド部
- 1104 TSデコーダ部
- 1105 AVデコーダ部
- 1106 コントロール部
- 1107 メモリ部
- 1108 ディスプレイインタフェース
- 201 第1のSTB
- 202 第2のSTB
- 203 第NのSTB
- 204～207 ネットワーク
- 208 送出センター
- 209 送信部
- 2001 LAN I/F

19/19

301 リボケーションリスト統合部

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/004138

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2000-261472 A (Toshiba Corp., Toshiba A.V.E. Kabushiki Kaisha), 22 September, 2000 (22.09.00), All pages; all drawings (Family: none)	7, 8, 15, 16 1-6, 9-14
X Y	JP 11-205305 A (Sony Corp.), 30 July, 1999 (30.07.99), All pages; all drawings & EP 930556 A2	7, 8, 15, 16 10-14
Y	Supervised by Hiroshi FUJIWARA, Hiroshi YASUDA, edited by Multi Media Tsushin Kenkyukai, "Point Zukaishiki Broadband + Mobile Hyojun MPEG Kyokasho", Ascii Corp., 11 February, 2003 (11.02.03), pages 317 to 320	1-6, 9-14

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
23 June, 2004 (23.06.04)Date of mailing of the international search report
06 July, 2004 (06.07.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/004138

Box No. II Observations where certain claims were found unsearchable (Continuation of Item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The technical feature common to claims 1-16 relate to "transmission or reception of revocation information". However, this technical feature is not novel since it is disclosed in JP 2000-261472. There exists no special technical feature common to claims 1-16.

Claims 1-6 and 9-14 relate to packetizing revocation information, multiplexing it on the stream, and sending the stream.

claims 7, 8, 15, and 16 relate to reception and storing of the revocation information.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, H04N7/16

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl.⁷ G06F12/14, H04N7/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2004年
日本国実用新案登録公報 1996-2004年
日本国登録実用新案公報 1994-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-261472 A (株式会社東芝, 東芝エー・ブイ・イー株式会社)	7, 8, 15, 16
Y	2000.09.22, 全頁, 全図 (ファミリーなし)	1-6, 9-14
X	JP 11-205305 A (ソニー株式会社)	7, 8, 15, 16
Y	1999.07.30, 全頁, 全図 & EP 930556 A2	10-14

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

23.06.2004

国際調査報告の発送日

06.7.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

高橋 克

5 N

3 0 4 4

電話番号 03-3581-1101 内線 3585

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	藤原 洋, 安田 浩 監修, マルチメディア通信研究会 編, "ポイント図解式 ブロードバンド+モバイル標準MPEG教科書", 株式会社アスキー, 2003.02.11, pp. 317-320	1-6, 9-14

第II欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第III欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲1-16に共通する事項は、「リボケーション情報を送信又は受信すること」であるが、この事項は特開2000-261472号に記載されているように周知であるから、請求の範囲1-16に共通する特別な技術的特徴はない。

請求の範囲1-6及び9-14は、リボケーション情報をパケット化し、ストリームに重複し、ストリームを送出することに関するものである。

請求の範囲7, 8, 15及び16は、リボケーション情報を受信し、記憶することに関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。